C:\Mark\SBIR-CDSAVV\FinalDemo\Scenes\Scene_Temp_EventWall_PxT_Class.wrl - Microsoft Internet Explorer

File   Edit   View   Favorites   Tools   Help

Back   Forward   Stop   Refresh   Home   Search   Favorites   History   Mail   Print   Edit

Address   C:\Mark\SBIR-CDSAVV\FinalDemo\Scenes\Scene_Temp_EventWall_PxT_Class.wrl   Go

Walk   Pan   Turn   Roll   Goto   Study

Time can be shown as a point, duration
or relative sequence

Event class

Line shows specific time each event
occurred on the targeted host

Time (hours)

12am 1   2   3   4   5   6   7   8   9   10   11   12pm

Packet Insertion

Packet Interception

IEmail   Classes of

Inventory Hosts   Vulnera-

Inventory Services   bilities &

Inventory Users   Attacks

Services Access

User and Group Accounts

Application Access

System File Access

Network Access

Denial of Service

Access Permission

Sniffing

Security Setup

Impersonation

Encryption

Firewall

Event
Type, 8

Attack
sources

Target Host's Location

Target Host's Organization

Hanscom Loc. 13
Hanscom Loc. 43
Surveillance
Command and Control
Medical
Mission Planning
Logistics
Intelligence
Hanscom Loc. 28
Hanscom Loc. 24
Hanscom Loc. 07
Hanscom Loc. 33
Hanscom Loc. 42

FIG. 1

My Computer

B1

C:\Mark\SBIR-CDSAV\FinalDemo\Scenes\Scene_Temp_EventWall_PxT_Class.wrl - Microsoft Internet Explorer

File   Edit   View   Favorites   Tools   Help

Back   Forward   Stop   Refresh   Home   Search   Favorites   History   Mail   Print   Edit

Address   C:\Mark\SBIR-CDSAV\FinalDemo\Scenes\Scene_Temp_EventWall_PxT_Class.wrl   Go

Walk

Pan

Turn

Roll

Goto

Study

FIG. 2

Event Type, 8

Time (hours)

11   10   9   8   7   6   5   4   3   2

Event class

Packet Scanners
Portal Interrogation
Grab
Inventory Vaults
Inventory Scanners
Inventory Users
Service Access
Users and Group Accounts
Application Access
Registry / File Access
Network Access
Denial Of Service
Access Permissions
Sniffing
Security Series
Interpretation
Encryptor
Flood

Attack Sources and the Times
That They Strike or
Sensors Reporting the Events

16

22

20

Attack sources

Rear plane of
temporal display
showing times that
specific attackers are
active

Organization

Hanscom Loc.
Hanscom Loc. 33
Hanscom Loc. 24
Hanscom Loc. 07

Attack sources

My Computer

FIG. 3

C:\Mark\SBIR-CDSAV\FinalDemo\Scenes\Scene_Temp_EventWall_PxT_Class.wrl - Microsoft Internet Explorer

File   Edit   View   Favorites   Tools   Help

Back   Forward   Stop   Refresh   Home   Search   Favorites   History   Mail   Print   Edit

Address   C:\Mark\SBIR-CDSAV\FinalDemo\Scenes\Scene_Temp_EventWall_PxT_Class.wrl   Go

Walk   Pan   Turn   Roll   Goto   Study
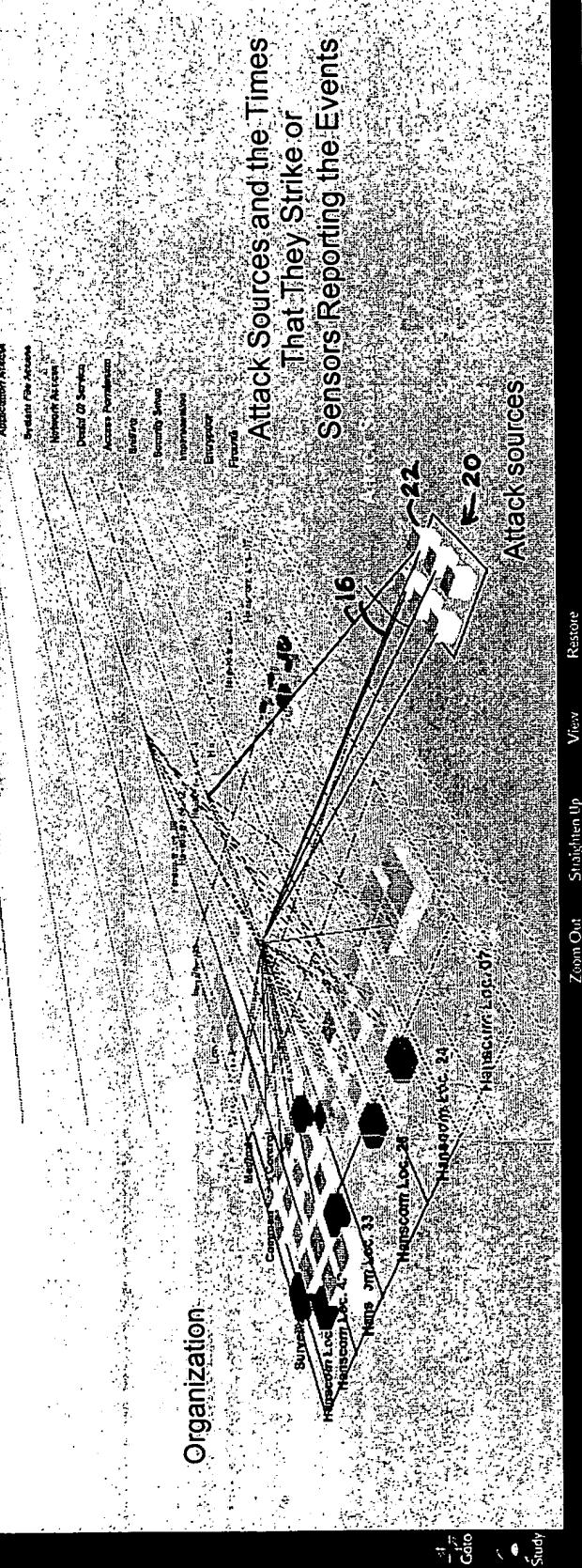
Zoom Out   Straighten Up   View   Restore

My Computer

Time (in hours)

Lines Show Time
That Target Host
Were Hit

Attacker Information
(Could Also be Reporting Sensors)

Attack sources

Location:
Hanscom loc: 47,

Target Hosts

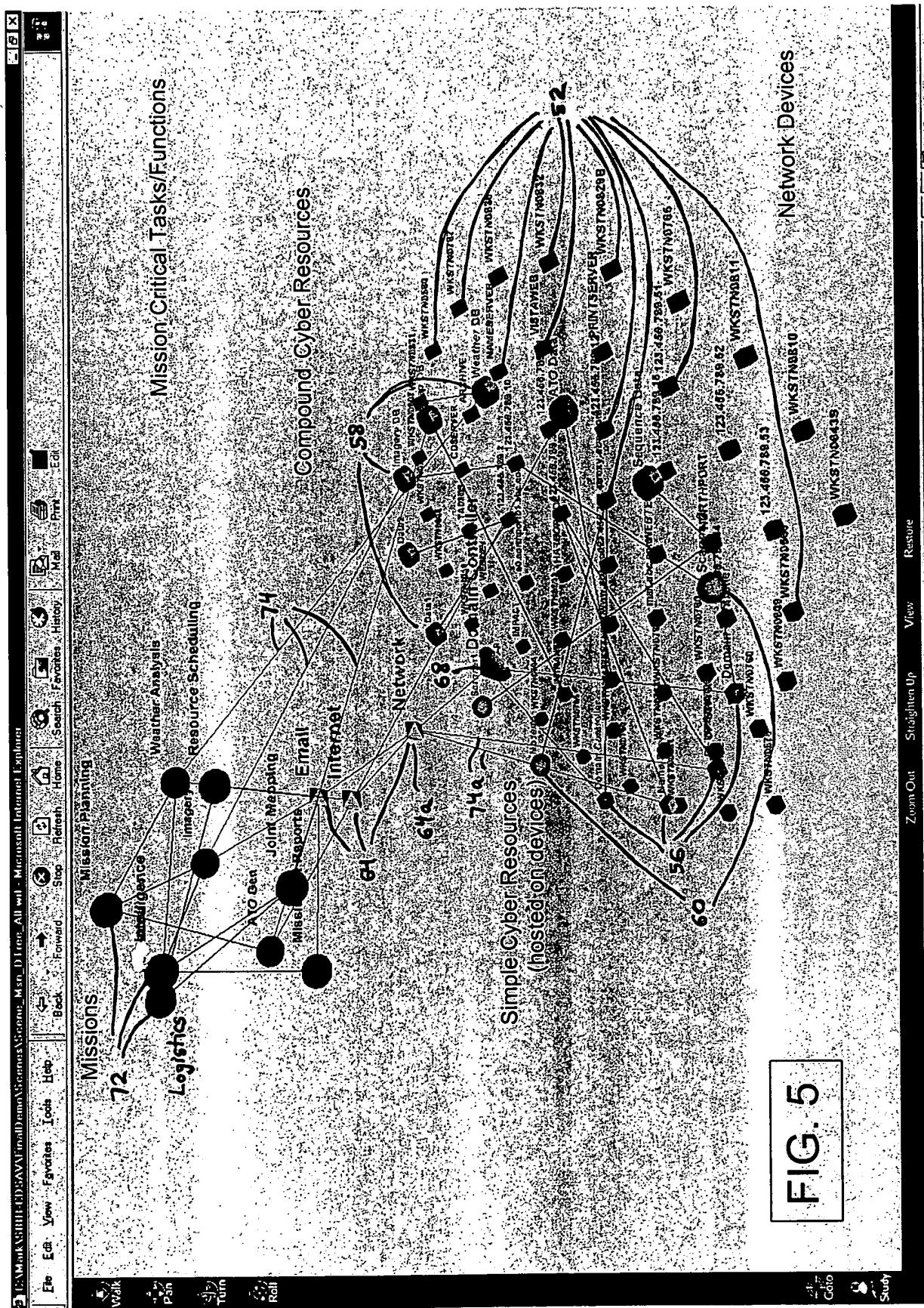Organizations: Intelligence, Logistics, Mission Planning, Medical, Command and Control, Surveillance

FIG. 4

BEST AVAILABLE COPY

BRMFS1 29395ov3
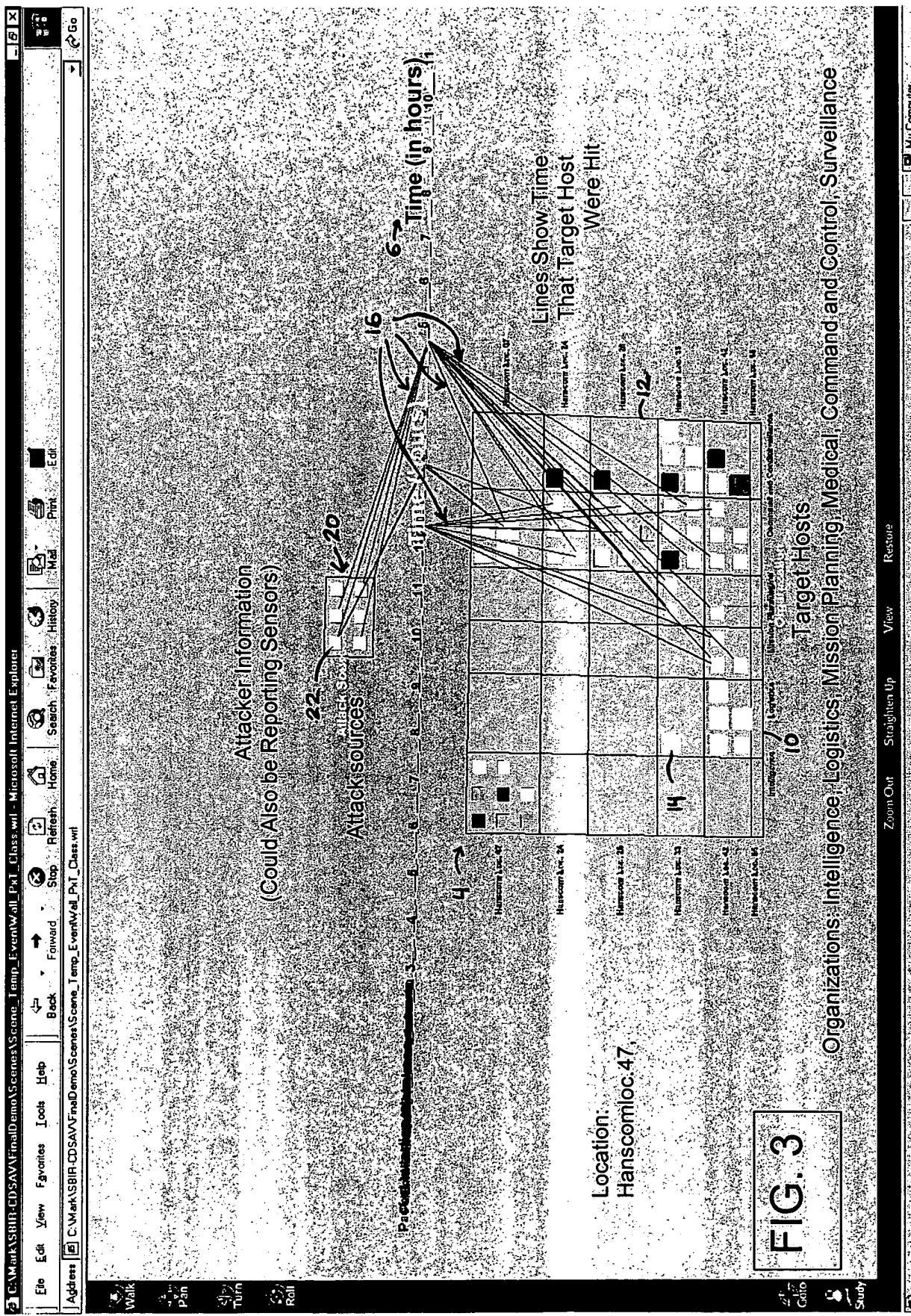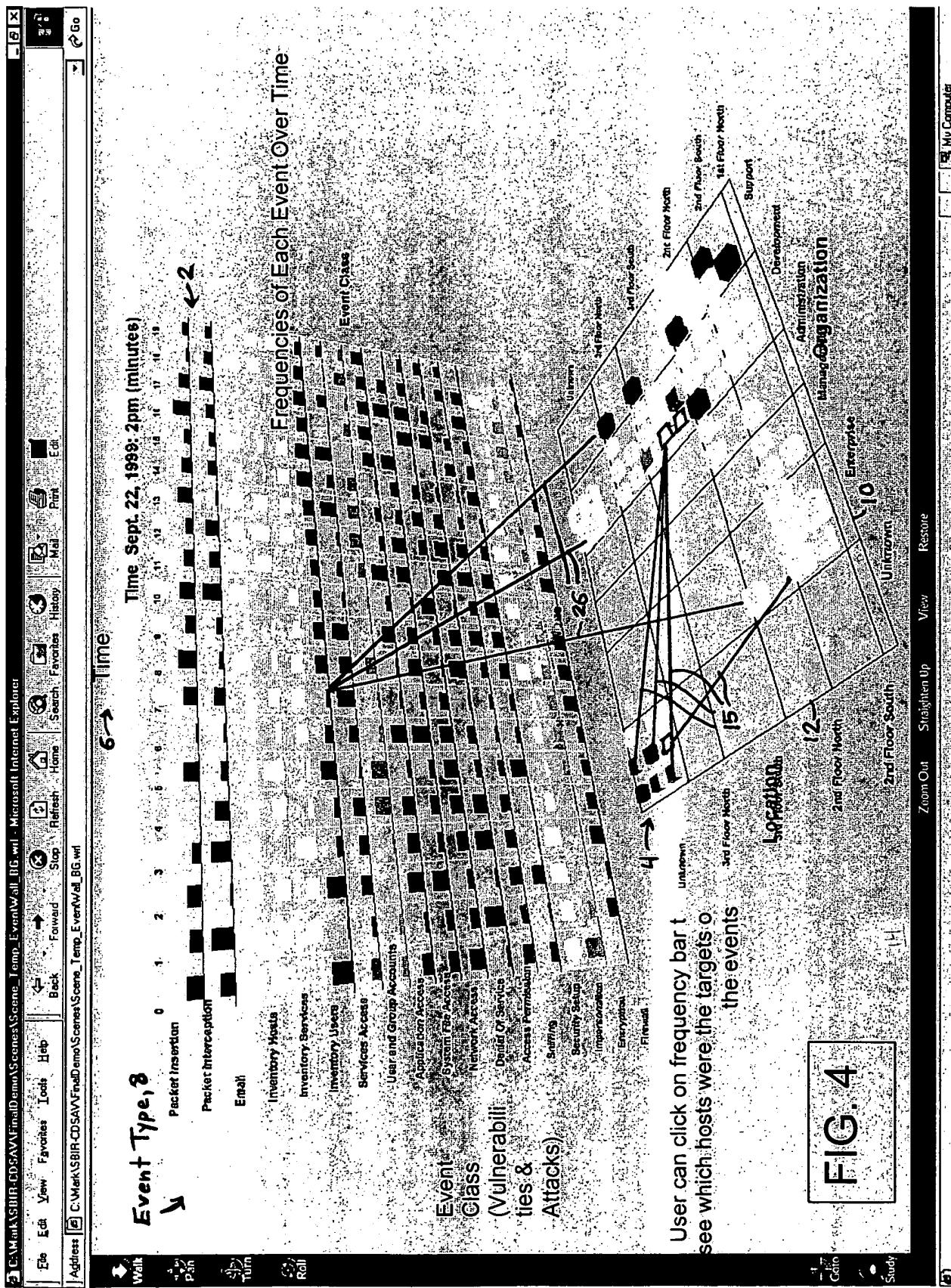
FIG. 5

BEST AVAILABLE COPY

FIG. 6

Missions associated with selected device

Mission-critical tasks dependent on that device

A device is selected by the user, based on its characteristics (e.g. OS, location, organization) or vulnerabilities

Compound cyber resources to which that device contributes (e.g. e-mail)

Resource created by device

Surveillance

Command and Control

Medical Facilities

Mission Utilities

Logistics

Intelligence

Hanscom Loc. 07
Hanscom Loc. 24
Hanscom Loc. 26
Hanscom Loc. 33
Hanscom Loc. 42
Hanscom Loc. 55